Investment protection
for open, integrated automation.
Industrial Security

industrial SECURITY

SIEMENS

integration

Data communication. Reliable, robust and secure.

One of the keys to greater productivity in industry.

The aim: greater security in production.

The means: minimize your risks.

Why does data transmission suddenly take so long?

Data transmission is disrupted. An immediate check is the top priority. To find acute weak points or defects, in this case action should be taken straight away.

What should be done in the event of an acute virus attack?

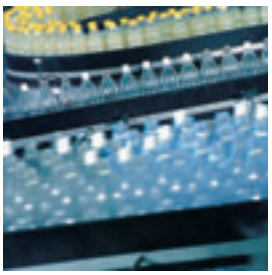
If an attack has occurred: Take steps immediately. Systematically and according to plan. In future, regulated processes for targeted measures will be a fixed part of future-proof network and automation concepts.

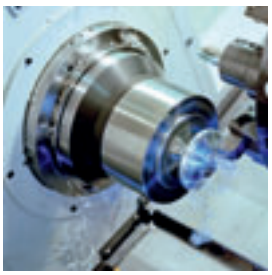
Is my data really safe from unauthorized access?

Increase data security. By minimizing risk. Better to start doing so today. No-one can guarantee 100% protection. Siemens offers plenty of ways, though, to ensure that risks are kept as negligible as possible. Our principle: a holistic approach and suitability for swift implementation.

What can be done to minimize risks in the long term?

Minimize risks in the long term. Best of all throughout the lifecycle of the plant. From planning, through engineering, right up to the daily use of products and systems. Security integrated from Siemens is holistic and targeted at the long term. Assistance with updates and general support and service worldwide are all part of this.






Can't you simply take proven security measures from the office and apply them in the factory?

Data security in the factory. Interaction between individual features and the system.
Production networks have to meet specific requirements, not the same as office networks. This is reflected in the network architecture and the nature of the software and hardware components that are used – designed for industry. Siemens also consistently makes use of its experience in automation for developments in Industrial Security.

But aren't data security measures complicated and expensive, and don't they hamper production?

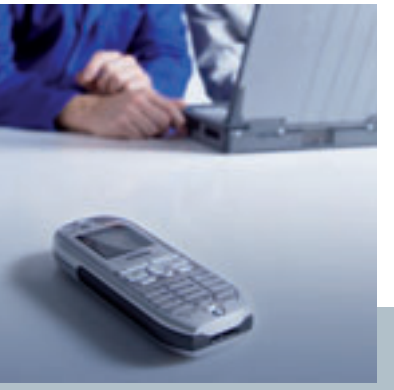
Increasing data security can be simple. Best example: SCALANCE S security modules. They are easy to implement and to apply without adverse effects. Reduced-risk data traffic is then possible within the secured zone. Also in isochronous real time.

How can the data network in production be secured?

Production with a secured data network. A great benefit for the whole company.
Production outages can be expensive. Likewise if management becomes more difficult because of disruptions to the flow of information. Undesirable manipulations from outside or also inside your company are a matter for Industrial Security from Siemens. The focus always remains on the reliability of the production processes and the flow of information in all areas of the enterprise.

Can automated installations be protected retrospectively?

It is quite possible to retrofit protection. That, too, will protect your investment.
SCALANCE S modules are not dependent on specific protocols. This means they can be integrated into the existing infrastructure without difficulty. But being part of Industrial Security also means that products and systems from Siemens support the possibility of convenient online upgrading. To make sure your protection always stays up to date, and therefore effective.



Office and production.
Better together.

Controlling your machines, monitoring your production lines, coordinating entire production areas – without automation and the necessary data communications to go with it, mastering these tasks would be inconceivable today. Open, consistent and uniform system technology has proved it brings advantages in terms of greater efficiency in all fields. But requirements continue to rise: the need to act more quickly, respond better to changes, increase productivity, and so on. To be able to carry on meeting these requirements in future and therefore also survive in the market, a company's processes all have to grow more closely together. One consequence of acknowledging this is the growing degree of networking of data communications in production areas with the corporate network.

Totally Integrated Automation.
And everything that goes with it.

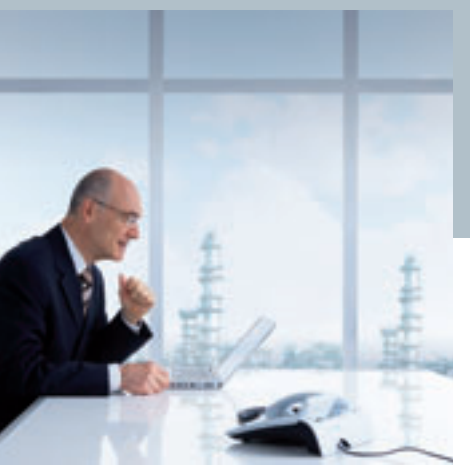
Siemens Automation and Drives offers products, systems and solutions for automation that allow horizontal and vertical consistency across all parts of an operation. Industrial communications with SIMATIC NET plays a leading role in this.

Industrial Ethernet networks.
Unity makes you strong.

Ethernet first established itself as an international standard, IEEE 802.3, for office networks. Siemens counts among the pioneers who made it possible to apply the benefits of the standard to industrial processes too. SIMATIC NET is one of the drivers of the Industrial Ethernet evolution. For networks – designed for industry. Armed with all the details to cope reliably with rising volumes of data, even in demanding circumstances.

Industrial Security.
To match IT integration.

Common structures and technologies have made not only engineering but also operation and service more efficient. For example, the use of web technology is now an indispensable part of many solutions. The adaptation of Ethernet to become Industrial Ethernet takes account of the specific conditions surrounding industrial processes. Accompanying the migration of IT and production automation, though, questions concerning the risks are now also increasingly the same. The answer from Siemens is: Industrial Security.



know-how

Industrial Security. Wherever you use automation.

To ensure consistent protection of your investment.

As openness and consistency continue to increase, the risk of unwanted manipulation also grows. This is why a security concept is needed that on the one hand offers reliable protection for industrial communication but on the other also takes account of the specific requirements of automation technology. Siemens faces up to this challenge in the industrial world with Industrial Security. So that your investment will also stay protected in the future.

Industrial Security.
The breadth on offer.

Whether it is a matter of rectifying a specific problem or minimizing potential risks – Siemens offers you an answer to every industrial security concern in industrial companies with open and consistent automation.

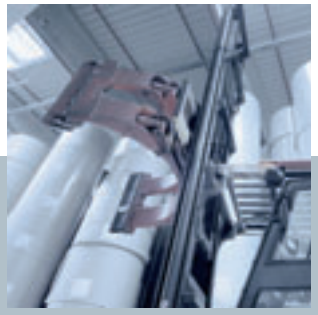
- **Robust components**
  Beginning at the development stage and then later in demanding tests, Siemens makes sure that the automation components have a general ruggedness about them. One aspect of this is IP hardening. In critical situations this can effectively prevent the destruction of a component.

- **Secured applications.**
  Interaction of vital details.
  Especially in the process industry, where some sequences are highly complex, automation technology finds itself caught between the need to offer optimum solutions to security requirements and the obligation to ensure economic operation.

Example: SIMATIC PCS 7
PCS 7 is the innovative process control system that, being part of Totally Integrated Automation, both supports openness and consistency to provide greater transparency and gives comprehensive protection against unintentional or targeted attacks on the plant operator's IT systems. With PCS 7, Industrial Security means the coordinated interaction of several individual measures such as encryption or firewalls and a defense-in-depth security architecture.

Example: SIMATIC Logon
User management with SIMATIC Logon is part and parcel of the Industrial Security concept. Logon is integrated into the security system and the Windows user administration functions, and thus meets the requirements of the Food and Drug Administration (FDA), whose rules and recommendations serve as a model for many fields and in particular in the pharmaceutical industry and the food sector are obligatory requirements.

Example: SINUMERIK 840 D
If machine tools need to be accessible from a remote location via the Internet for service purposes, once again, appropriate protection is required. In SINUMERIK controllers, precautions have therefore been taken. Firewall mechanisms are already integrated.



- **Security products**
  Using products originally created for IT security, such as SCALANCE S modules, you set up secured zones and thereby also safeguard products which do not have their own protection from being manipulated.

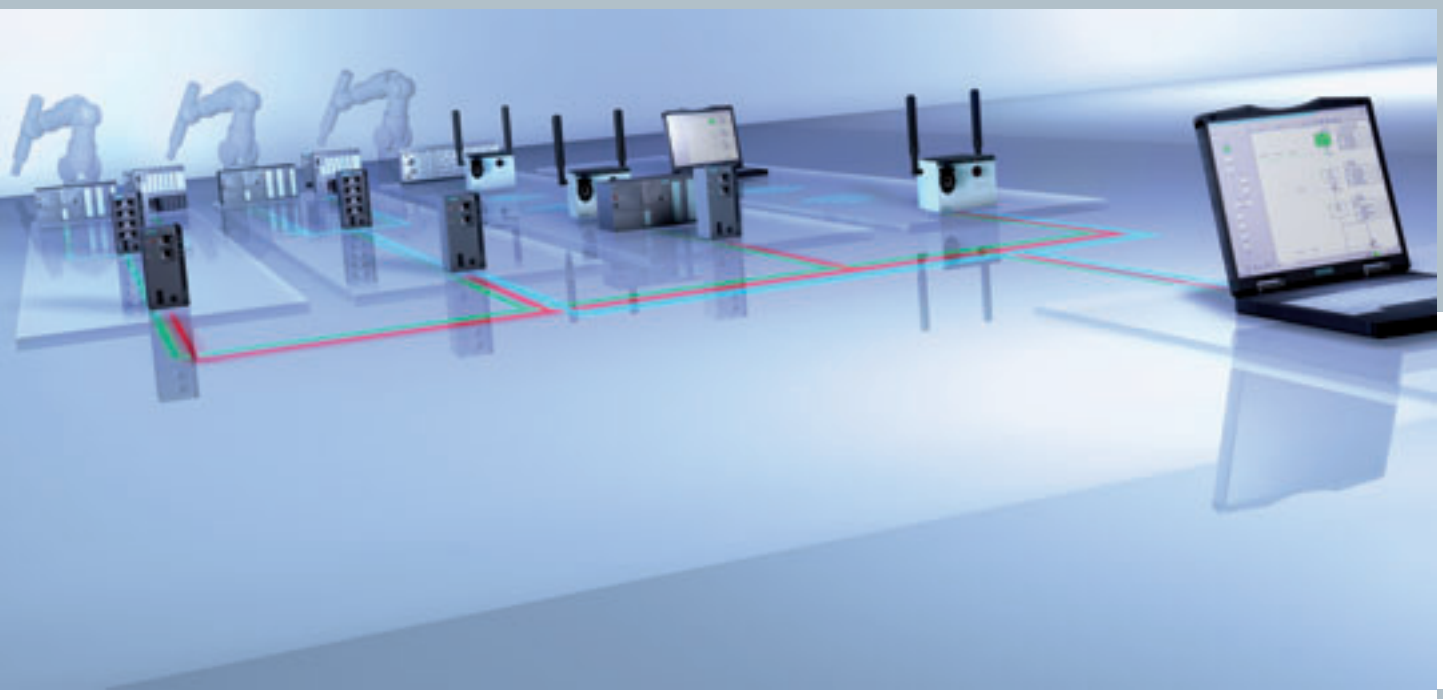
- **Security service and support**
  Siemens supports you through all phases of the lifecycle: in the analysis and optimization of existing plants, in new design concepts, in implementation and during operation.

Standards instead of expensive one-off solutions.

Our aspiration in relation to security is similar to that in safety technology with Safety Integrated for the personnel and plant protection: enabling the implementation of highly effective solutions in an efficient way.

International standardization.

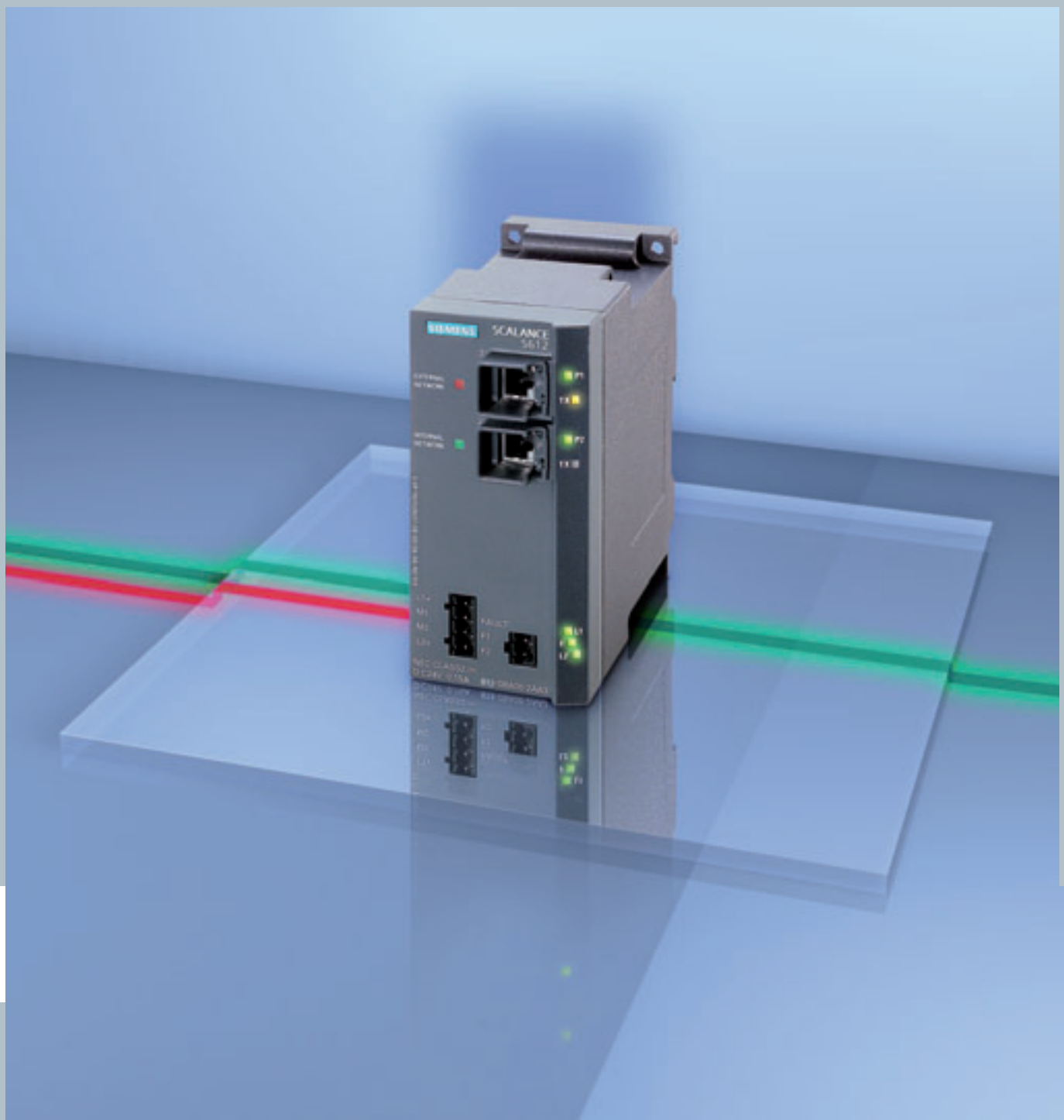
Siemens commits substantial energy to the creation of internationally applicable security standards and the prevention of the emergence of contradictory local guidelines. Siemens' participation in relevant committees, associations and certain institutes, such as IEC 62443 (Security for industrial process measurement and control – Network and system security); ISA SP99 (Manufacturing and Control Systems Security) or VDI Guideline 2182 (Information security of automated machines and plants), helps to ensure that Industrial Security can also be put into practice reliably and efficiently in future.

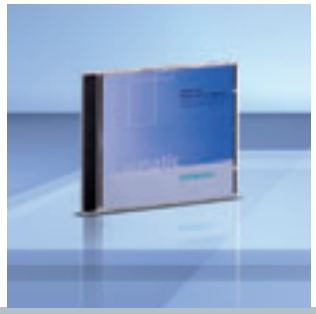


standards

Security concept. Flexible. Reaction-free.

Protokol-independent. Simple to implement.





Security client software

Scalable security with the SCALANCE S module family

SCALANCE is the new product generation for building Industrial Ethernet networks. High levels of performance, availability and flexibility for future networks were just as much an objective as the achievement of an up-to-date and future-proof means of protecting a network. The result: SCALANCE X.
A full range of switches for a huge variety of tasks. SCALANCE W. Components with innovative details for entirely new industrial wireless LAN concepts. SCALANCE S. Security modules for appropriate protection of new and existing industrial networks. All of these components satisfy the quality standards set for SIMATIC NET: designed for industry. From particularly sturdy casings all the way through to convincing details.

Virtual private networks. In industry too. With SCALANCE X.

A high degree of protection, IP65, strong securing collars at the ports, optical fiber technology and high-speed redundancy management are among the highlights of the SCALANCE X Industrial Ethernet switches. Up-to-date network management (SNMP) plays just as big a part in reliable data communications as the possibility of setting up virtual private networks (VPN). The current range also offers you Layer 3 switches in addition to devices for Layer 2.

Wireless networks with security. SCALANCE W.

Antenna diversity, reservation of data rates, rapid roaming, innovative RCoax antenna technology and wireless transfer – even of critical process data – count among the benefits of SCALANCE W when true Industrial Wireless LAN structures need to be set up, with no room for compromise. WPA and a range of other techniques of encrypting the wirelessly transmitted data assist in the provision of security just as much as the perfect interaction with wire-bound Industrial Ethernet networks.

Industrial Security for all parts of a plant. SCALANCE S.

Along with protection of a local network from external threats by firewalls, in the complex network architecture of manufacturing industry it is just as important to provide protection within an automation cell.
If automation components are unable to protect themselves, the innovative SCALANCE security module concept is the right choice: SCALANCE S modules are especially designed for use in automation engineering, but link smoothly to the security structures of the office and IT world. Through the combination of various security precautions such as firewalls and VPN via IPsec tunnels, these modules provide protection against data espionage, data manipulation, unauthorized access and automated intrusion attempts.
Installed networks can be upgraded with no adverse effects within a short space of time and at minimum expense. The SCALANCE S modules thus offer crucial benefits for both the investor and the user.

Benefits of Industrial Security with SCALANCE S and SOFTNET Security Client

- No expert knowledge required, nor constant maintenance
- Security on behalf of devices without their own protective function
- Ability to be integrated into existing networks without adverse effects
- Protection of individual automation cells simple to implement
- Protection of real-time domains without impairment of performance
- Minimal configuration work
- Adaptations can be implemented quickly as needs change
- Certificates generated automatically by configuring tool
- Minimal expenditure on project planning

dimensions

For high performance, high availability, plant and personnel protection.

Industrial Security. For different needs.

Every industry has its own priorities which determine the conceptual design of the automation systems and the networks that are integrated into them: coping with high peak or continuous loads, sustained availability, protection of recipes, obligations to pro-vide documentation and verification, and the protection of personnel, equipment or the environment. Many of these requirements are also either directly or indirectly linked to protection against unwanted or unauthorized manipulation. Moreover, specific standards and in some cases statutory regulations and official recommendations have a part to play in determining the choice and nature of the technical equipment and how it is handled.

For secured applications. Security features, tools and products.

Within an application there are a huge range of details that provide for Industrial Security.

Examples:

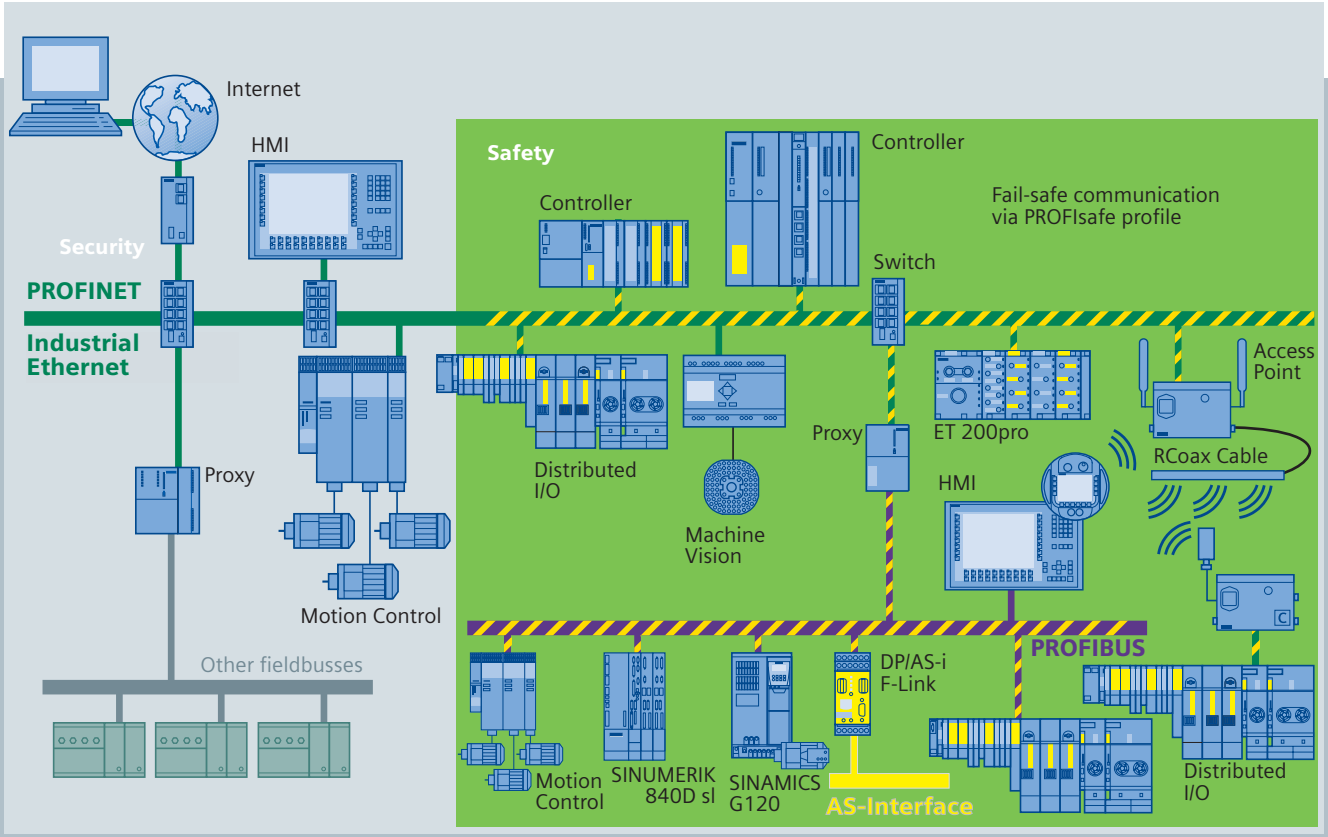
SIMATIC Logon
Logon is used in the environment of the SIMATIC WinCC visualization software, and by providing a whole series of security mechanisms it offers advantages such as:

- Time-saving, central, cross-plant user management, integrated into Windows User Management
- High levels of security on the administrator and user sides
- Suitability for single-user and client/server systems
- High availability through primary/secondary domain controllers and integration into local Windows User Management

SIMATIC ADDM.
Tool for backup and restore
SIMATIC ADDM is a uniform tool for SIMATIC, SINUMERIK, drives, operator panels and PCs, thus offering a great many advantages:

- Time saving thanks to centralized, automatic data backup
- Greater plant availability through fast data restoration when replacing modules
- Greater data availability through high levels of data security on the central server
- Increased data security thanks to data archives with version and user rights administration

Secured motion control.
Mit SINUMERIK
Industrial Security is also provided for with SINUMERIK, the controllers perfected for machine tools. For example, the PCU of SINUMERIK 840 D is available as a high-security desktop in accordance with the Microsoft Windows XP Security Guide, equipped with an active Windows XP firewall. The NCUs for Linux are equipped with an active Linux packet filtering firewall.

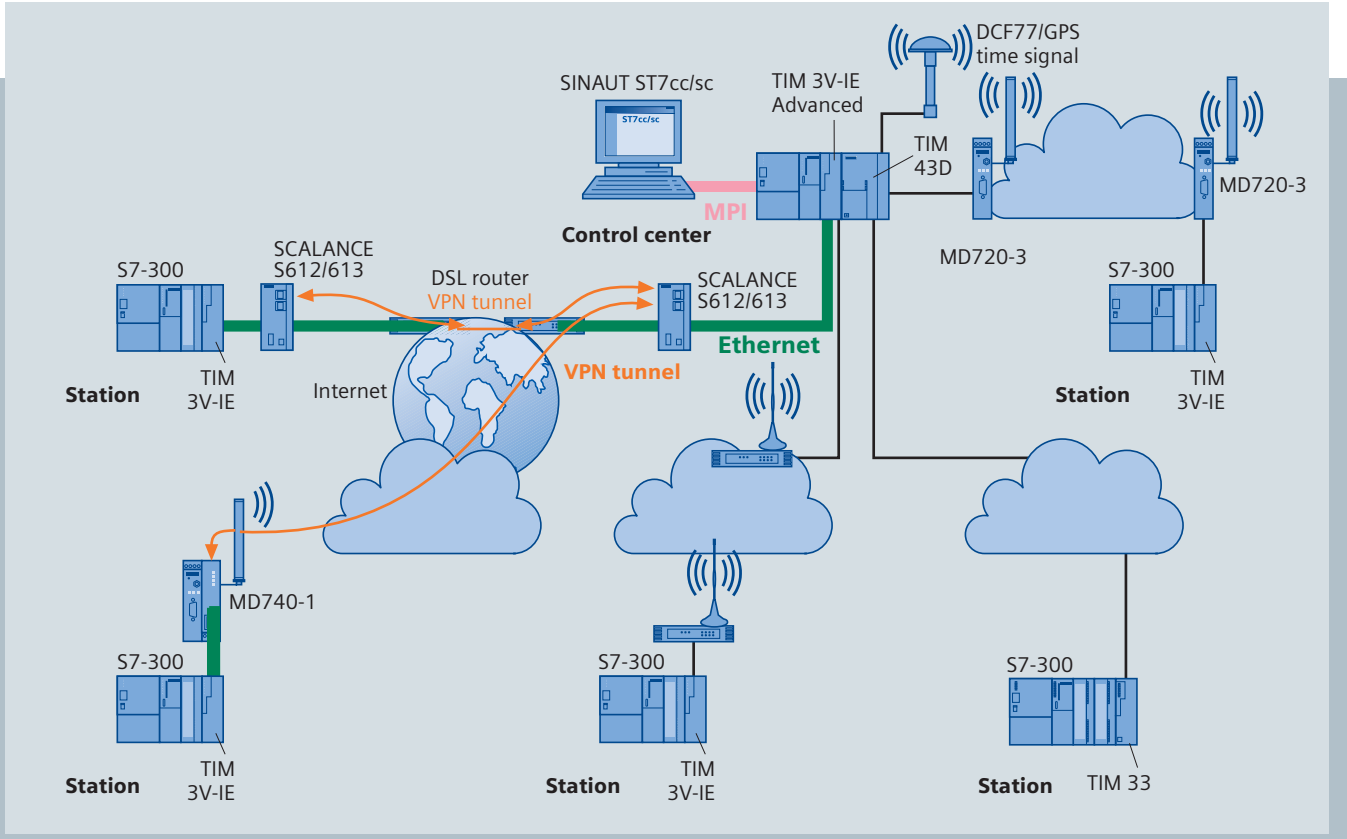


Industrial Security. Also the basis for the protection of people and equipment

Siemens offers innovative technology for future-proof concepts to protect both humans and machines by paying equal attention to safety and efficiency. PROFIsafe is part of the comprehensive range under the umbrella of Safety Integrated for safety-oriented applications on the basis of PROFIBUS or Ethernet-based networking with PROFINET.

Ethernet, being an open, uniform structure with a connection to the Internet, calls for corresponding security mechanisms.

The solution: With SCALANCE S, the security modules from Siemens, it is easy to create secured PROFIsafe zones in which the safety-oriented system can reliably perform the required tasks.



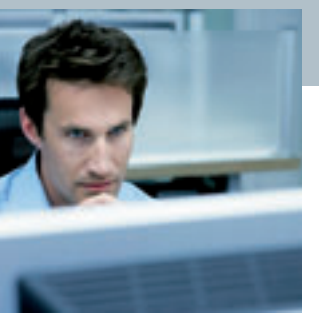
Industrial Security. Integration in SINAUT telecontrol.

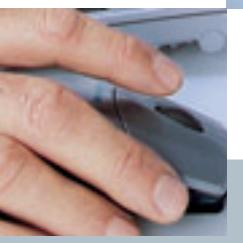
Whether in small automation applications, large-scale system architectures or even remote stations connected over long distances via telecontrol – Siemens always offers you the opportunity of implementing future-proof Industrial Security solutions.

Another example is SINAUT: This multi-faceted system for telecontrol duties is based on SIMATIC and enables components to be networked across a wide area network (WAN). For data transmission, among other things SINAUT uses WAN based on Ethernet technology, such as broadband systems or the Internet.

Virtual private network. In SINAUT telecontrol this is built in.

When you are using a GPRS network, the telecontrol system's control center PC must be reachable at all times. Permanent Internet links, for example via DSL, are particularly efficient. The necessary data security is provided by the creation of a virtual private network (VPN): With SINAUT, data is transmitted in both directions between the control center and the GSM/GPRS modems in the remote stations via a secure VPN tunnel. The SINAUT connection manager also allows internode communication between the stations via SINAUT's own VPN.

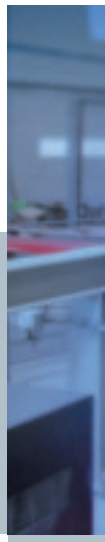




confidence

Products, systems and solutions. Open, uniform and safe.

With the integration of Industrial Security.



Having open and consistent data communications offers many advantages for both investors in and users of automation solutions. However, using Ethernet and Internet technology means there is a need for security measures to protect the data traffic and the data itself. Such requirements will increase yet further in future, and affect all areas of a company – from the world of the office through to manufacturing and logistics.

The range on offer. Industrial Security included.

Siemens offers you a varied range of products, systems and solutions designed for open and consistent communications. This also includes offering a corresponding range of products and services to provide comprehensive protection for those applications.

The need for applications to be safe from unwanted manipulation is in some cases the object of statutory provisions and recommendations. For those products and systems to which this applies, Siemens sees to it that they can protect themselves accordingly.

However, self-protection is not possible in all cases, and for various reasons it does not always make sense either. This is one of the reasons why Siemens developed tools and components that are able to take care of protection for other devices as well. One innovative example of this is SCALANCE S, the security modules. The fact that existing installations can also be protected efficiently and effectively with these – and without detrimental effects – is an advantage both for the user on the shop floor and for the investor.

Protection. Only effective with tangible action.

A variety of possible ways of integrating security into innovative concepts, problem-free implementation without specialist knowledge and without disproportionate expenditure on training, smooth operation and efficient service – these are guiding principles in the constant further development of our products and motivation behind what we do. So that your company is safely protected in all its parts, along with your facilities and installations through all phases of their lifecycle.

Industrial Security. A joint task.

For communication and automation to be open, transparent and safe, for products, systems and solutions to be able to meet these requirements effectively and at the same time efficiently, in all branches of industry and into the future – that is the purpose of our research and development, and equally of our participation in relevant associations, committees and official bodies, not to mention the intensive cooperation with our customers wherever they are in the world.

Integration from the very beginning.

Do you want to restructure your IT world? Are you planning to modernize your automation or do you intend to rebuild a production facility? Seize the opportunity and consider the use of appropriate security products. Integrate Industrial Security into your concept from the very beginning. Act now, and talk to us. We will be happy to advise you. Please look on the Internet to find the details of the appropriate person at Siemens Automation and Drives to contact. Go to:
www.siemens.com/automation/partner

For Industrial Security. Act now!

We will be happy to advise you. The contact details for a partner from Siemens Automation and Drives near you are available on the Internet:
www.siemens.com/automation/partner

Details about SCALANCE network components:
www.siemens.com/scalance

The latest news about PROFINET:
www.siemens.com/profinet

Further information on the subject of industrial communication:
www.siemens.com/simatic-net

You can also find other information brochures and technical descriptions on our Internet pages, by clicking on Support.

www.siemens.com/industrial-security

PUBLICIS

Subject to changewithout prior notice 04/07 | Order No. E20001-A410-P820-V1-X-7600 | DISPO 06366 | 2100/3132 fbc 147.0703 MK.PT.IK.ALLG.52.7.09 WS 03072. | Printed in Germany |

Siemens AG
Automation and Drives
Industrial Automation Systems
P.O. Box 4848
90327 NUREMBERG
GERMANY

www.siemens.com/automation